PIERRE-CYRILLE HÉAM

A lower bound for reversible automata

*Informatique théorique et applications*, tome 34, n° 5 (2000), p. 331-341

<http://www.numdam.org/item?id=ITA_2000__34_5_331_0>
A LOWER BOUND FOR REVERSIBLE AUTOMATA

PIERRE-CYRILLE HÉAM

Abstract. A reversible automaton is a finite automaton in which each letter induces a partial one-to-one map from the set of states into itself. We solve the following problem proposed by Pin. Given an alphabet $A$, does there exist a sequence of languages $K_n$ on $A$ which can be accepted by a reversible automaton, and such that the number of states of the minimal automaton of $K_n$ is in $O(n)$, while the minimal number of states of a reversible automaton accepting $K_n$ is in $O(p^n)$ for some $p > 1$? We give such an example with $p = \left(\frac{3}{2}\right)^{\frac{1}{12}}$.

Résumé. Un automate réversible est un automate fini dans lequel chaque lettre réalise une fonction injective de l’ensemble des états dans lui-même. On résout dans cet article le problème suivant posé par Pin : étant donné un alphabet $A$, existe-t-il une suite de langages $K_n$ sur $A$ qui peuvent être reconnus par un automate réversible, et tels que le nombre d’états de l’automate minimal de $K_n$ soit en $O(n)$ alors que le nombre minimal d’états d’un automate réversible reconnaissant $K_n$ soit en $O(p^n)$ avec $p > 1$ ? On donne un tel exemple avec $p = \left(\frac{3}{2}\right)^{\frac{1}{12}}$.

AMS Subject Classification. 68Q45, 68Q70.

INTRODUCTION

In this paper we answer an open question on reversible automata proposed by Pin in [10]. Reversible automata form a natural class of automata with links to artificial intelligence [1], and to biprefix codes [4]. Moreover reversible automata are used to study inverse monoids, inverse automata [12,13] and certain topological problems [7,10,12,13]. We prove that computing a reversible automaton which
recognizes a language given by its minimal automaton can not be done, in some cases, faster than in exponential time (if the alphabet contains at least two letters).

We denote by \(|K|\) the cardinality of a set \(K\).

We assume that the reader is familiar with the basic definitions on words and formal languages. For more information we refer the reader to [2]. Let us denote by \(|u|\) the length of a word and by \(u^\sim\) its mirror.

Let us recall that a finite automaton is a 5-tuple \(A = (Q, A, E, I, F)\) where \(Q\) is a finite set of states, \(A\) is the alphabet, \(E \subseteq Q \times A \times Q\) is the set of edges (or transitions), \(I \subseteq Q\) is the set of initial states and \(F \subseteq Q\) is the set of final states. A path in \(A\) is a finite sequence of consecutive edges:

\[
p = (q_0, a_0, q_1), (q_1, a_1, q_2), \ldots, (q_n-1, a_n, q_n).
\]

The label of the path \(p\) is the word \(a_1 a_2 \cdots a_n\), its origin is \(q_0\) and its end is \(q_n\). A word is accepted by \(A\) if it is the label of a path in \(A\) having its origin in \(I\) and its end in \(F\). The set of words accepted by \(A\) is denoted by \(L(A)\). For every state \(q\) and language \(K\), we denote by \(q.K\) the subset of \(Q\) of all the states which are the end of a path having its origin in \(q\) and its label in \(K\). An automaton is said to be trim if for each state \(q\) there exists a path from an initial state to \(q\) and a path from \(q\) to a final state. An automaton is deterministic if it has a unique initial state and does not contain any pair of edges of the form \((q, a, q_1)\) and \((q, a, q_2)\) with \(q_1 \neq q_2\). An important result of automata theory states that for an automaton \(A\) there exists exactly one (up to isomorphism) deterministic automaton with a minimal number of states which accepts the same language as \(A\). It is called the minimal automaton of \(L(A)\). A reversible automaton is a finite automaton in which each letter induces a partial one-to-one map from the set of states into itself. It also is an automaton which does not contain any pair of edges of the form \((q, a, q_1)\) and \((q, a, q_2)\) with \(q_1 \neq q_2\) or \((q_1, a, q)\) and \((q_2, a, q)\) with \(q_1 \neq q_2\). It may happen that a reversible automaton is not deterministic because it may have several initial states. Reversible automata were studied by Pin [10] and by Silva [11]. For an automaton \(A = (Q, A, E, I, F)\), let us introduce the following languages, for \(p\) and \(q\) in \(Q\):

\[
L_{p,q}(A) = \{u \in A^* \mid p.u = q\}.
\]

If \(I = \{i\}\), we write \(L_p(A)\) for \(L_{i,p}(A)\), and if \(F = \{f\}\) we write \(R_q(A)\) for \(L_{q,f}(A)\). If there is no ambiguity we just write \(L_{p,q}, L_p\) and \(R_q\).

For a language \(L\) which is recognized by a reversible automaton we introduce two invariants: \(m(L)\), the number of states of its minimal automaton and \(c(L)\) the minimal number of states of a reversible automaton accepting \(L\). We denote by \(r(n)\) and \(R(n)\) the following functions:

\[
r(n) = \min\{c(L) \mid m(L) = n\} \quad \text{and} \quad R(n) = \max\{c(L) \mid m(L) \leq n\}.
\]

It is proved in [10] that \(r(n) = O\left(\frac{\ln n}{\ln \ln n}\right)^2\). Let us remark that \(R(n)\) is an increasing function of \(n\). We prove here that \(R(n) = \Omega(\rho^n)\) for some \(\rho > 1\).
1. Main theorem

Theorem 1.1. The relation \( R(n) = \Omega(\rho^n) \) holds with \( \rho = \left( \frac{3\sqrt{2}}{4} \right)^{\frac{1}{n}} \approx 1.001 \) if the alphabet contains at least two letters.

For the proof, let us consider the language \( L = \{aa, ab, ba\} \) on the alphabet \( A = \{a, b\} \). Before we proceed, let us note the following technical result.

Lemma 1.2. Let \( A = (Q, A, E, i, F) \) be a reversible trim automaton accepting a non-empty subset of \( L = \{aa, ab, ba\} \). For each state \( s \in Q \), let \( L_s \) be the set of words which can be read from state \( i \) to \( s \). Then one of the following holds:

(a) \( |F| = 3 \) and \( |L_s| = 1 \) for each state \( s \in F \);
(b) \( |F| = 2 \), \( F = \{s_1, s_2\} \), \( |L_{s_1}| = 2 \) and \( |L_{s_2}| = 1 \);
(c) \( |F| = 2 \) and \( |L_s| = 1 \) for each state \( s \in F \);
(d) \( |F| = 1 \), \( F = \{s\} \) and \( |L_s| = 2 \);
(e) \( |F| = 1 \), \( F = \{s\} \) and \( |L_s| = 1 \).

Proof. First we observe that in a reversible automaton on 2 letters, each state is the origin (resp. the end) of at most 2 transitions. Since \( |L| = 3 \) and \( A \) is trim, \( F \) has at most 3 elements, and if \( |F| = 3 \), then \( |L_s| = 1 \) for each final state \( s \), that is (a) holds.

If \( |F| = 2 \), say \( F = \{s_1, s_2\} \), then \( |L_{s_1}| + |L_{s_2}| \leq 3 \). Since \( A \) is trim \( |L_s| > 0 \) for every state, so (b) or (c) holds.

Finally, let us assume that \( F = \{s\} \) is a singleton. We need to verify that \( |L_s| \neq 3 \), that is, \( A \) does not accept all of \( L \). If there is no \( a \)-labeled transition out of \( i \), then \( L_s = L(A) = \{ba\} \) and (e) holds. If there is no \( b \)-labeled transition out of \( i \), then \( L_s \subseteq \{ab, aa\} \) and (d) or (e) holds. We now consider the case where both an \( a \)-labeled transition and a \( b \)-labeled transition start in state \( i \). If \( i.a = i.b \), then there is no \( b \)-labeled transition from \( i.a \) to the final state \( s \) since \( bb \) cannot be accepted, and hence \( L_s = \{aa, ba\} \) and (d) holds. On the other hand, suppose that \( i.a \neq i.b \). Since \( A \) is trim, there is an \( a \)-labeled transition from state \( i.b \) to \( s \). But \( A \) is reversible, so there is no \( a \)-labeled transition from state \( i.a \) to \( s \), and the word \( aa \) is not accepted. In particular, \( L_s = \{ab, ba\} \) and (d) holds. \( \square \)

For every integer \( n \), \( L^n \) is a finite language which can be recognized by a reversible automaton (it is easy to check that every finite language can be recognized by a reversible automaton). We prove that \( c(L^{2n}) \geq \rho^n \), while \( m(L^{2n}) = O(n) \).
First observe that, for every positive integer \( n \), \( |L^n| = 3^n \), \( L^n = (L^n)^\sim \), and every word of \( L^n \) has length \( 2n \). Furthermore it is easy to check that the minimal automaton recognizing \( L^n \) is the following one:

Thus the minimal automaton of \( L^n \) has \( m(L^n) = 3n + 1 \) states. Moreover, if \( A \) is a trim automaton which recognizes a sub-language of \( L^n \), then for all pairs of states \( p \) and \( q \) of \( A \), all the words of \( L_{pq} \) have the same length.

Let \( A = (Q, A, \varepsilon, \{i\}, \{f\}) \) be a reversible automaton with a unique initial state and a unique final state recognizing a sub-language of \( L^{2n} \). Let \( M(A) = i.A^{2n} \) be the set of states of \( A \) we can reach from \( i \) by reading a word of length \( 2n \) (half of the length of the words of \( L^{2n} \)).

**Proposition 1.3.** With the above notation, the following relation holds

\[
|L(A)| \leq \frac{1}{2} \left( \sum_{q \in M(A)} |L_q|^2 + |R_q^\sim|^2 \right).
\] (1)

**Proof.** By definition we have:

\[
L(A) = \bigcup_{q \in M(A)} L_q R_q.
\]

But \( A \) is deterministic and hence, if \( p \neq q \) then \( L_p \cap L_q = \emptyset \). Consequently, if \( p, q \in M(A) \) then \( L_p R_p \cap L_q R_q = \emptyset \). Indeed the prefix of length \( 2n \) of a word of \( L_p R_p \cap L_q R_q \) would have to be in \( L_p \cap L_q \). Thus we get:

\[
|L(A)| = \sum_{q \in M(A)} |L_q||R_q|.
\]

Since \( R_q \) is finite we have \( |R_q| = |R_q^\sim| \). But for every pair of real numbers \( (x, y) \) we have \( xy \leq \frac{1}{2}(x^2 + y^2) \). From this we deduce (1). \( \square \)

For the next proposition and the next three lemmas we consider a reversible automaton \( A = (Q, A, \varepsilon, \{i\}, F) \) recognizing a sub-language of \( L^n \) (where \( n \) is a
strictly positive integer), and having a unique initial state \( i \). For every state \( q \) of \( Q \) let us denote by \( n_q \) the cardinal of \( L_q \).

**Proposition 1.4.** The following equality holds:

\[
\sum_{q \in F} n_q^2 \leq 8^n. \tag{2}
\]

To prove Proposition 1.4 we proceed by induction on \( n \) and we need some technical lemmas. For the proof we can assume without loss of generality that \( A \) is trim.

**Lemma 1.5.** If \( n = 1 \), Proposition 1.4 is true.

**Proof.** Applying Lemma 1.2 to \( A \), we get:

- In case (a), \( \sum_{q \in F} n_q^2 = |L_{i,s_1}|^2 + |L_{i,s_2}|^2 + |L_{i,s_3}|^2 = 3 \).
- In case (b), \( \sum_{q \in F} n_q^2 = |L_{i,s_1}|^2 + |L_{i,s_2}|^2 = 4 + 1 = 5 \).
- In case (c), \( \sum_{q \in F} n_q^2 = |L_{i,s_1}|^2 + |L_{i,s_2}|^2 = 1 + 1 = 2 \).
- In case (d), \( \sum_{q \in F} n_q^2 = |L_{i,s_1}|^2 = 4 \).
- In case (e), \( \sum_{q \in F} n_q^2 = |L_{i,s_1}|^2 = 1 \).

This completes the proof. \( \square \)

We denote by \( S \) the set of states which we can reach by reading a word of length \( 2n - 2 \) (every word of \( L^n \) has length \( 2n \)).

**Lemma 1.6.** For every \( q \in F \) we have

\[
n_q = \sum_{s \in S} n_s |L_{s,q}|. \tag{3}
\]

**Proof.** Since every word of \( L(A) \) has length \( 2n \) we have

\[
L_q = \bigcup_{s \in S} L_s L_{s,q}. \tag{4}
\]

But \( A \) is deterministic, so as in the proof of Proposition 1.3 the union in (4) is disjoint. Since \( n_q = |L_q| \) for every state \( q \) in \( Q \), we can now deduce formula (1.6) from formula (4). \( \square \)

We now prove that:

**Lemma 1.7.** For all \( s \in S \) we have

\[
\sum_{q \in F} \sum_{t \in S} |L_{s,q}| |L_{t,q}| \leq 8. \tag{5}
\]
Proof. Let \( s \in S \) and let \( F_s \) be the set of states in \( F \), which we can reach from \( s \). If \( q \in F \), we denote by \( I_q \) the set of states of \( S \) from which \( q \) can be reached. The sum in formula (5) is in fact equal to

\[
\sum_{q \in F_s} \sum_{t \in I_q} |L_{s,q}||L_{t,q}|.
\]

Since \( A \) is trim, the words which can be read from a state in \( S \) to a state in \( F \), are all in \( L \). Moreover, as \( A \) is reversible, if \( q \in F \), then the languages \( L_{t,q} (t \in I_q) \) are pairwise disjoint and hence

\[
\sum_{t \in I_q} |L_{t,q}| \leq 3.
\]

Consider the automaton obtained from \( A \) by first making \( s \) the initial state and then trimming. This automaton satisfies the hypothesis of Lemma 1.2 and one of the following five cases arises.

(a) \( |F_s| = 3 \) and \( |L_{s,q}| = 1 \) for each \( q \in F_s \).

We have, say, the following configuration

Note that there is no state \( t \in I_{q_1} \) such that \( t.b = s.a \): if there was, we would have \( t.bb = q_2 \), so \( bb \in L_{t,q_2} \subset L \), a contradiction. Since \( A \) is trim, it follows that \( ba \notin \bigcup_{t \in I_{q_1}} L_{t,q_1} \) and hence

\[
\sum_{t \in I_{q_1}} |L_{t,q_1}| \leq 2.
\]

We already observed that

\[
\sum_{t \in I_{q_2}} |L_{t,q_2}| \leq 3 \quad \text{and} \quad \sum_{t \in I_{q_3}} |L_{t,q_3}| \leq 3
\]

so

\[
\sum_{q \in F_s} \sum_{t \in I_q} |L_{s,q}||L_{t,q}| = \sum_{q \in F_s} \sum_{t \in I_q} |L_{t,q}| \leq 2 + 3 + 3 = 8.
\]
(b) $F_s = \{q_1, q_2\}$ with $|L_{s,q_1}| = 2$ and $|L_{s,q_2}| = 1$. Since $A$ is reversible we have either $I_{q_1} = \{s\}$ or $I_{q_1} = \{s, u\}$ with $|L_{u,q_1}| = 1$.

(b1) If $I_{q_1} = \{s\}$ we have

$$\sum_{t \in I_{q_1}} |L_{t,q_1}| |L_{s,q_1}| = 4$$

and

$$\sum_{t \in I_{q_2}} |L_{t,q_2}| |L_{s,q_2}| = \sum_{t \in I_{q_2}} |L_{t,q_2}| \leq 3$$

so

$$\sum_{q \in F_s} \sum_{t \in I_s} |L_{s,q}| |L_{t,q}| \leq 4 + 3 = 7.$$ 

This case can be illustrated in the following figure:

(b2) Assume that $I_{q_1} = \{s, u\}$. By reversibility, we have $L_{u,q_1} = L \setminus L_{s,q_1}$. Since $|L_{s,q_1}| = 2$, it follows that $|L_{u,q_2}| = 1$ and

$$\sum_{t \in I_{q_1}} |L_{s,q_1}| |L_{t,q_1}| = 2 (|L_{s,q_1}| + |L_{u,q_1}|) = 6.$$ 

If $I_{q_2} = \{s\}$, we are finished:

$$\sum_{q \in F_s} \sum_{t \in I_q} |L_{s,q}| |L_{t,q}| = 6 + 1 = 7.$$ 

In order to go further, let us analyze this situation in more detail. If $L_{s,q_1} = \{aa, ba\}$, then by reversibility we have $s.b = s.a$. Moreover in that case $L_{s,q_2} = \{a\}$, so that $(s.a).b = q_2$. This implies in turn that $s.bb = q_2$, $bb \in L_{s,q_2}$, a contradiction.
Now if $L_{s,q_1} = \{aa, ab\}$ then by determinism both the $a$-labeled and the $b$-labeled transitions into $q_1$ come from $s.a$. Moreover $L_{u,q_1} = \{ba\}$, so $u.b = s.a$ and we now have $u.bb = q_1$, $bb \in L_{u,q_1}$, again a contradiction.

Thus $aa \notin L_{s,q_1}$ and we have $L_{s,q_1} = \{ab, ba\}$, $L_{s,q_2} = L_{u,q_1} = \{aa\}$ and the following configuration

Suppose that $v \in I_{q_2}$, $v \neq s$. Then $aa \notin L_{v,q_2}$ by reversibility. Also $ba \notin L_{v,q_2}$; otherwise $v.b = s.a$ and $v.bb = q_1$. This implies $bb \in L_{v,q_1} \subseteq L$, a contradiction. Thus if $v \neq s$ lies in $I_{q_2}$, then $L_{v,q_2} = \{ab\}$. This shows that

$$\sum_{t \in I_{q_2}} |L_{s,q_2}||L_{t,q_2}| = \sum_{t \in I_{q_2}} |L_{t,q_2}| \leq 2$$
and hence
\[ \sum_{q \in F_s} \sum_{t \in I_q} |L_{s, q}||L_{t, q}| \leq 8. \]

(c) \(|F_s| = 2\) and \(|L_{s, q}| = 1\) for each \(q \in F_s\). Since \(\sum_{t \in I_q} |L_{t, q}| \leq 3\) for each \(q \in F\), we have
\[ \sum_{q \in F_s} \sum_{t \in I_q} |L_{s, q}||L_{t, q}| = \sum_{q \in F_s} \sum_{t \in I_q} |L_{t, q}| \leq 2 \times 3 = 6. \]

(d–e) \(F_s = \{q\}\) and \(|L_{s, q}| = 2\) (resp. \(1\)). Again using that \(\sum_{t \in I_q} |L_{t, q}| \leq 3\), we find that
\[ \sum_{q \in F_s} \sum_{t \in I_q} |L_{s, q}||L_{t, q}| \leq 6 \text{ (resp. 3).} \]

Now we can prove Proposition 1.4.

Proof. We proceed by induction on \(n\). The proposition is true for \(n = 1\) by Lemma 1.5.

Assume now that it is true for \(n\). Let \(A = (Q, A, E, \{i\}, F)\) be a reversible trim automaton with a unique initial state \(i\) recognizing a subset of \(L^{n+1}\). According to Lemma 1.6
\[ n_q^2 = \sum_{(s, t) \in S^2} n_s n_t |L_{s, q}||L_{t, q}|. \]

Thus we have:
\[ \sum_{q \in F} n_q^2 = \sum_{q \in F} \sum_{(s, t) \in S^2} n_s n_t |L_{s, q}||L_{t, q}| = \sum_{(s, t) \in S^2} \left( \sum_{q \in F} |L_{s, q}||L_{t, q}| \right) n_s n_t \]
\[ \leq \frac{1}{2} \sum_{(s, t) \in S^2} \left( \sum_{q \in F} |L_{s, q}||L_{t, q}| \right) n_s^2 + \frac{1}{2} \sum_{(s, t) \in S^2} \left( \sum_{q \in F} |L_{s, q}||L_{t, q}| \right) n_t^2 \]
\[ \leq \sum_{(s, t) \in S^2} \left( \sum_{q \in F} |L_{s, q}||L_{t, q}| \right) n_s^2. \]

From this, by Lemma 1.7, we have
\[ \sum_{q \in F} n_q^2 \leq 8 \sum_{s \in S} n_s^2. \]
Now we can apply the induction hypothesis to the automaton deduced from \( A \) by taking \( S \) for the set of final states rather than \( F \), and by making it trim. We obtain:

\[
\sum_{s \in S} n_s^2 \leq 8^n.
\]

This establishes the proposition.

Now we prove the main theorem.

Proof. Let \( n \) be a positive integer and let \( A = (Q, A, E, I, F) \) be a reversible automaton recognizing \( L^{2n} \). For each \( i \in I \) and \( f \in F \) let us denote by \( A_{if} \) the automaton \((Q, A, E, \{i\}, \{f\})\).

It is clear that

\[
L(A) = \bigcup_{i \in I, f \in F} L(A_{if}).
\]

According to formula (1) we have

\[
|L(A_{if})| \leq \frac{1}{2} \left( \sum_{q \in M(A_{if})} |L_q(A_{if})|^2 + |R_q(A_{if})|^2 \right).
\]

Now the reversible automata \((Q, A, E', \{f\}, M(A_{if}))\) recognizes a sublanguage of \( L^n \). By formula (2), we have

\[
\sum_{q \in M(A_{if})} |L_q(A_{if})|^2 \leq 8^n.
\]

Moreover, let us denote by \( E' = \{(p, a_i, q) \mid (q, a_i, p) \in E\} \). The reversible automata \((Q, A, E', \{f\}, M(A_{if}))\) also recognizes a sublanguage of \( L^n \), and by (2), we have

\[
\sum_{q \in M(A_{if})} |R_q(A_{if})|^2 \leq 8^n.
\]

Thus, \( |L(A_{if})| \leq 8^n \) by formula 8.

By formula (7), it comes \( |L(A)| \leq |I||F|8^n \). But \( |L(A)| = 9^n \), so

\[
|I||F| \geq \left( \frac{9}{8} \right)^n.
\]

It follows that \( I \) or \( F \) contain a least \( r^n \) elements with \( r = \frac{3\sqrt{2}}{4} \). Since \( I \) and \( F \) are subsets of \( Q \) we have \( |Q| \geq r^n \).

We have proved that \( c(L^{2n}) \geq r^n \). But \( m(L^{2n}) = 6n + 1 \). Hence \( R(6n + 1) = \Omega(r^n) \) and, since \( R(n) \) is an increasing function of \( n \), this proves the theorem with \( \rho = \frac{r^\frac{1}{8}}{8} \). □
The author wishes to express his thanks to J.-E Pin for suggesting the problem, to C. Nicaud for helpful comments, and to P. Weil for his active interest in the preparation of this paper.

REFERENCES


Communicated by J.-E. Pin.

Received February 9, 2000. Accepted September 29, 2000.